REMARKS

The courtesy of Examiners Pwu and Nooristany in granting a telephone interview on February 20, 2008 to attorney Edward Callan is sincerely appreciated. During the interview the arguments presented herein with respect to claim 9 were discussed. The Examiner's response to such arguments is discussed below with reference to the traversal of the claim rejections under 35 USC 102. No agreement was reached as to the allowability of the claims.

Claim 9 is amended.

Claim Rejections - 35 USC 102

The rejection of claims 9-20 and 25-28 under 35 USC 102(b) as being anticipated by US patent 6,249, 805 to Fleming is respectfully traversed for at least the following reasons:

Fleming teaches a computer system and method for filtering unauthorized electronic mail messages that are sent by senders to a user. The system includes a list of the identifications of the senders who are authorized to send an electronic mail message to the user. When an electronic mail message is received, the system determines whether the sender of the electronic mail message is authorized by determining whether the identification of the sender in the electronic mail message is in the list of the identifications of the senders who are authorized. When the sender of the electronic mail message is determined to be authorized, the system stores the electronic mail message in an Inbox folder. When the sender of the electronic mail message is determined to be not authorized, the system stores the electronic mail message in a Junk Mail folder. In this way, the electronic mail messages are automatically stored in the appropriate folder based on whether the sender is authorized so that the user can view the Inbox folder containing the electronic mail messages sent by authorized senders separately from the Junk Mail folder containing the electronic mail messages sent by unauthorized senders.

Claim 9 is not anticipated by Fleming because Fleming does not disclose the feature recited in the last paragraph of this claim, to wit:

> "performing an analysis to see if there is serial, incremental user identification occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system".

In the rejection of claim 9, the Examiner supports his assertion that this feature is disclosed by Fleming, by stating, "The authorization component intercepts electronic mail messages that are sent to a user before they are placed in the user's Inbox folder – Col. 4, lines 25-16 [*sic*]; 'Note, i.e. Authorization component acts as the same as the above performance for analysis'."

Col. 4, lines 16-25 of Fleming, states,

> "The authorization component intercepts electronic mail messages that are sent to a user before they are placed in the user's Inbox folder. The authorization component has the identifications of all senders who are authorized to send electronic mail messages to the user. When an electronic mail message is intercepted, the authorization component retrieves the identification of the sender from the envelope portion of the intercepted electronic mail message. The authorization component then determines whether the retrieved identification of the sender matches the identification of one of the authorized senders."

Neither the quoted portion of Fleming nor any other portion of Fleming that Applicant could find discloses or suggests the above-quoted feature recited in the last paragraph of claim 9.

In response to Applicant pointing in the Remarks portion of the Amendment filed August 29, 2007 that there was no support in Fleming for the feature recited in the last paragraph of claim 9, the Examiner asserted,

> "Fleming teaches 'performing an analysis (authorization component) to see if there is user identification occurring so that conclusions can be drawn concerning

automatic attempts at breaking into the email system' (i.e., The authorization component intercepts electronic mail messages that are sent to a user before they are placed in the user's Inbox folder, hence, authorization component acts as the same as the above process 'performing an analysis' in which the system recognizes and filters out all user's [*sic*] based on their identity before they breaking [*sic*] into the email system). This means that the process of identifying of an unauthorized sender must include serial, incremental identification of user because consecutive (serial), increasing (incremental) identifying of an unauthorized user would draw to the same conclusion."

The Examiner's assertion here cannot be sustained because:

- Fleming does not disclose or suggest that his authorization component recognizes and filters out all users based on their identity before they break into the email system.
- Fleming makes no suggestion whatsoever of performing an analysis that enables conclusions to be drawn concerning automatic attempts at breaking into the e-mail system.
- Fleming's disclosure of intercepting electronic mail messages that are sent to a user before they are placed in the user's Inbox folder does not support the Examiner's assertion that the authorization component recognizes and filters out all users based on their identity before they break into the email system.
- Fleming's disclosure of intercepting electronic mail messages that are sent to a user (at Col 4, lines 16-25, quoted above), merely describes retrieving the identification of the sender from the envelope portion of the intercepted electronic mail message and then determining whether the retrieved identification of the sender matches the identification of one of the authorized senders. Such disclosure of identifying senders and determining whether they are authorized senders does not support the Examiner's assertion that Fleming's authorization component filters out all users based on their identity before they break into the email system.

- Fleming's authorization component identifies senders. In order to identify senders in accordance with Fleming's disclosure, it is not necessary to perform an analysis to see if there is serial, incremental user identification occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system, as required by claim 9.

During the interview Examiners Pwu and Nooristany did not rebut these points of argument. However, they refused to withdraw the final rejection for the following reason: The step recited in the last paragraph of claim 9, to wit: "performing an analysis ..." does not appear to be related to either the other recited steps of the method or the subject matter recited in the preamble, to wit: a method to automatically handle undesired electronic mail...". The examiners stated that for this reason, claim 9 should have been rejected under 35 USC 112.

Applicant's representative responded to the examiners' above-indicated reason for refusing to withdraw the final rejection by stating that claim 9 could be amended so that the step of "performing an analysis was recited "in combination with" the method recited in the preceding portion (lines 1-8) of the claim. SPE Pwu replied by stating that even though such an amendment might overcome the above-indicated reason for refusing to withdraw the final rejection, another search of the prior art and further examination would be required, whereby in accordance with PTO rules, such an amendment would not be entered after final rejection. In addition, SPE Pwu requested that Applicant explain the relationship between the step of "performing an analysis ..." and the method to automatically handle undesired electronic mail recited in the preceding portion (lines 1-8) of claim 9.

Claim 9 is amended to recite that the step of "performing an analysis..." is "in combination with" the method recited in the preceding portion (lines 1-8).

The step of "performing an analysis to see if there is serial, incremental user identification occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system" is related to the recited "method to automatically

handle undesired electronic mail" in that by breaking into the e-mail system one can so modify the e-mail system as to enable an undesired e-mail to be stored in the mailbox MB by compromising the authentication aspect of the recited method required by the steps recited at lines 4-8, such as, for example, by adding the address of an undesired sender to the list of authorized sender addresses.

Claims 10-20 and 25-28 all depend from claim 9 and are believed to be patentable at least for the same reasons as is claim 9. Some of these claims are specifically discussed below.

Claims 11 and 12 are not anticipated by Fleming because Fleming does not disclose the feature recited in each of these two claims, to wit:

> "wherein the incoming e-mails are selectively put through an automatic handling and analysis process, which can be selectively configured by the recipient and by the ISP, selectively in the e-mail server, in a comparison device, and in at least one of the mailboxes, said process initiated and configured either on a case-by-case basis or permanently."

The portions of Fleming cited by the Examiner in rejecting claims 11 and 12 do not disclose or suggest selective configuration by the recipient and by the ISP of an automatic e-mail handling and analysis process, as required by these two claims. Also it is not seen where any other portion of Fleming discloses or suggests such selective configuration.

Claims 13-16 are not anticipated by Fleming because Fleming does not disclose the feature recited in each of these four claims, to wit:

> "wherein all executable programs sent as attachments to e-mails are automatically separated in the JMB."

The portions of Fleming cited by the Examiner in rejecting claims 13-16 do not disclose or suggest that all executable programs sent as attachments to e-mails are

automatically separated in the JMB, as required by these four claims. It cannot be inferred from Fleming's statement that "all electronic messages received from a certain sender can automatically be stored in a designated folder" that all executable programs sent as attachments to e-mails are automatically separated in the JMB. Fleming makes no mention of either executable programs, attachments to e-mails, or automatic separation in a junk mail folder of executable programs sent as attachments to e-mails, much less separation of all such attachments.

Claims 17-20 are not anticipated by Fleming because Fleming does not disclose the feature recited in each of these four claims, to wit:

> "wherein if an undesired e-mail is received, discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender."

The portions of Fleming cited by the Examiner in rejecting claims 17-20 do not disclose or suggest that discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender, as required by these four claims. Fleming merely states, "Whenever a recipient does not want to be included on a mailing list, the recipient can notify the de-spamming computer system." The de-spamming computer is not the sender. Fleming mentions the de-spamming computer in the following context:

> "A service, known as a 'de-spamming service,' has been provided that attempts to limit the junk mail that is sent. Such a de-spamming service maintains a list of the electronic mail addresses of users who have requested not to receive junk mail. When a promotional company wishes to send an electronic mail message to all the users whose electronic mail addresses are on its mailing list, the promotional company first sends the electronic mail messages to the de-spamming computer system. The de-spamming computer system checks its list of electronic mail addresses and deletes any of the electronic mail messages that are destined to any electronic mail addresses on its list. The de-spamming computer system then forwards the remaining electronic mail messages onto the recipients." (Column 3, lines 3-16)

The sender is the promotional company, not the de-spamming computer.

Claim Rejections – 35 USC 103

The rejection of claims 21-24 as being unpatentable under 35 U.S.C. 103(e) over US patent 6,249, 805 to Fleming in view of US Patent Application Publication No. 2002/0091776 by Nolan et al. is respectfully traversed for at least the following reasons:

Since claims 21-24 all depend from claim 9, Applicant submits that they are not unpatentable over by Fleming for at least the same reasons as set forth above explaining why claim 9 is not anticipated by Fleming.

> Nolan was cited as disclosing the subject matter recited in claims 21-24, to wit: "wherein virus checks of the e-mail can be carried out selectively at an established time of day or each time a message arrives."

However, the subject matter recited in these four claims cannot be inferred from the portion of Nolan cited by the Examiner, which merely states:

> "While it is accepted that email engine processors are well known, such as, those used in centralised email virus scanning, for example, an email virus scanning program sold under the trademark MIMESWEEPER, the systems such as MIMESWEEPER work on the gateway intercepting messages and checking them before the [*sic*] reach the email server."

Nolan makes no suggestion of the virus checks being carried out selectively at an established time of day or each time a message arrives. In the context of claim 9, upon which these four claims depend, the arrival of the message is at the receiver not at an email server. Further, Nolan fails to supply the limitation not present in or suggested by Fleming.

Conclusion

Applicant does not necessarily agree with any of the Examiner's comments regarding the applicability of the cited references to any of the claims. However, in view of the reasons presented herein for traversing the rejections of the claims, applicant is not presenting additional arguments at this time. Applicant reserves the right to present additional arguments for traversing the present and any future rejections of the claims.

Examination and allowance of claims 9-28 is respectfully requested.

Respectfully submitted,

Walter KELLER

By: Lawrence A. Maxham
Attorney for Applicant
Registration No. 24,483

The Maxham Firm
Attorneys At Law
9330 Scranton Road, Suite 350
San Diego, California 92121
Telephone: (858) 587-7659
Facsimile: (858) 587-7658